Section C - Description/Specifications/Statement of Work

This document provides funding for a severable service contract that crosses fiscal years in compliance with 10 U.S. Code 2410 (a). Therefore, the performance for the base year may not exceed September 26, 2020.

SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT

Work under this performance-based task order will be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein will be referred to as Performance Work Statement (PWS):

SHORT TITLE: DEFENSE HEALTH AGENCY CYBERSECURITY ASSESSMENT AND AUTHORIZATION SUPPORT

1.0 PURPOSE

The Department of the Navy (DoN) Naval Information Warfare Center Atlantic (NIWC Atlantic) Program Management Competency provides a diverse range of Program/Information Management and Information Technology (IM/IT) support services to multiple federal organizations; including the Defense Health Agency (DHA). DHA is comprised of all Medical Military Services, National Capital Region Medical Directorate (NCR-MD), and Military Health Systems (MHS) Cyber infrastructure Services (MCiS). NIWC Atlantic provides oversight, management controls, best practices, and continuous improvement processes for all projects executed under the DHA umbrella.

The DHA works closely with the major command surgeons, the MCiS, as well as the Departments of the Army, Navy, NCR-MD, and other governmental agencies to deliver medical service for more than 4.9 million eligible beneficiaries. DHA Health Information Technology (HIT) Directorate is responsible for providing Cybersecurity and authorization support for all the DHA organization.

1.1 SCOPE

NIWC Atlantic delivers Cybersecurity, systems engineering and support services to the DHA and the MHS community of interest. DHA is a Combat Support Activity (CSA) that directly supports the warfighter's medical readiness and includes all military medical facilities. This task will support the Cybersecurity and Risk Management Framework (RMF) initiatives, and provide support to the DHA Assessment and Authorization Division. NIWC Atlantic will execute Cybersecurity services to assist in ensuring compliance with Federal, Department of Defense (DoD), DHA and subservices regulations and policies. Additionally, NIWC Atlantic will ensure that the HIT performance is driven to maximum availability and efficiency through technically capable support teams with specialized knowledge, skills and experience supporting clinical applications and toolsets used by military health providers.

The objective of this Task Order (TO) is to assist NIWC Atlantic in project execution of Cybersecurity services at locations throughout the Contiguous United States (CONUS) and Outside the Contiguous United States (OCONUS) areas. This includes support to all DoD MHS sites, which vary in size from 1500 to over 60,000 server and workstation assets and support as many 430 Programs of Record Systems of varying size, architecture and operating systems.

1.1.1 <u>Multiple Funding</u>

This task order is funded with multiple appropriations. The RDT&E CLINs (2001, 2101, 2201, 2301) will be utilized for support of new systems that are pre-Milestone C in their program life cycle. As indicated in Section B and Section G, all PWS tasking is associated with each funding

CLIN.

2.0 PLACE(S) OF PERFORMANCE

2.1 GOVERNMENT FACILITIES

No Government facilities (i.e., office space or lab space) are provided on this task order. Work shall be performed at the contractor facility and/or temporarily at locations specified under travel.

2.2 CONTRACTOR FACILITIES

A significant portion of work issued under this task order requires close liaison with the Government. The contractor shall be prepared to establish a local facility within a thirty (30)-mileradius of NIWC Atlantic's facility located at 1 Innovation Drive, North Charleston, SC 29410-4200. Close proximity allows for proper task order administration duties. The contractor's facility is not necessary for the exclusive use of this task order and can be utilized on a shared basis. For task orders with Government Property, the contractor's facility shall include physical security to protect Government assets as identified in Para10.0. The contractor shall meet all facility location and size requirements within 30 days after task order award. Facility space shall include offices, conference rooms, lab work, and a staging area for materials and equipment.

For work performed outside of Government facilities, the Contractor may perform the required level of effort at an alternative worksite, provided the Contractor has a company-approved alternative worksite plan. The primary worksite is the traditional "main office" worksite. An alternative worksite means an employee's residence or a telecommuting center. A telecommuting center is a geographically convenient office setting as an alternative to an employee's main office. The Government reserves the right to review the Contractor's alternative worksite plan. In the event performance becomes unacceptable, the Contractor will be prohibited from counting the hours performed at the alternative worksite in fulfilling the total level of effort obligations of the contract. Regardless of the work location, all contract terms and conditions, including security requirements and labor laws, remain in effect. The Government shall not incur any additional cost nor provide additional equipment for contract performance as a result of the Contractor's election to implement an alternative worksite plan.

NOTE: Individuals designated as key personnel may perform a maximum of 25% of their labor hours at the alternative worksite.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list all required non-personal services tasks that will be required throughout the task order. The contractor shall provide necessary resources with knowledge and experience as cited in the personal qualification clause to support the listed tasks. Contractors shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) which does not include performance of inherently Governmental functions. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

The following paragraphs list all required support tasks that will be required throughout the contract life. The contractor shall provide necessary resources and knowledge to effectively support the listed tasks. Specific objectives will be dependent on the basic contract and the task order

(TO) written against the basic contract. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of cost, schedules, and resources.

In performance of this tasking, the contractor shall be required to utilize a government provided Windows 10 computing platform image.

3.1 RELEVANT EXPERIENCE

3.1.1 Systems and Equipment

The contractor shall provide functional and technical expertise testing, validating, and supporting a wide range of health related DoN and DoD Cybersecurity enabled systems. Systems will range from client-server applications employing interactive and batch processes to customized web-based solutions operating in a distributed or standalone environment. Such systems include, but are not limited to:

- Assured Compliance Assessment Solution (ACAS)
- Host Based Security System (HBSS) to include associated modules
- System Center Configuration Manager (SCCM)
- IP-based network enabled medical devices
- Enhanced Mitigation Experience Toolkit (EMET)
- Group Policy Objects (GPOs)
- Security Information Event Managers (SIEM)
- Intrusion detection and prevention systems (IDS and IPS)
- Network devices; including routers, firewalls, switches, and web proxies

3.1.2 Programs and Initiatives

The contractor shall have expertise supporting and complying with DHA and DoD enterprise Cybersecurity initiatives. Such programs and initiatives include at a minimum:

- Risk Management Framework (RMF)
- Vulnerability Remediation Asset Manager (VRAM)
- Continuous Monitoring and Risk Scoring (CMRS)
- Consolidated System Tracking and Reporting (CSTAR)
- Enterprise Mission Assurance Support Service (eMASS)

3.2 PROGRAM MANAGEMENT

The contractor shall assist the Government project manager providing support at the sponsor level.

3.2.1 Program Support

The contractor shall work closely with the government project manager supporting the needs of the program at the sponsor level. Requirements include coordinating meetings, preparing budget drills, developing agenda items and status briefings, attending high-level meetings, generating minutes, and tracking action items. Additionally, the contractor shall utilize analysis of actual outcomes or their expert opinion to recommend policies, doctrine, tactics, and procedures at the Federal, State, and Local level. Program support will require significant coordination and interface with various DoD and non-DoD activities located in and out of the CONUS.

3.2.2 Program Support Documentation

The contractor shall develop and draft various Program Management (PM) reports (CDRL T001). The following documents are typical PM deliverables that the contractor shall have knowledge writing:

- Cost Estimation
- DHA / Service RMF Program Cybersecurity budgeting
- Meeting Agenda and Minutes
- Plans of Action and Milestones (POA&M)
- Work Breakdown Structure (WBS) Alignment
- Accounting Classification Reference Number (ACRN) Alignment (e.g. Navy ACRN AA, NCR ACRN AB)
- Labor Hours Information
- Fully Burdened Rates
- Costs for Other Direct Costs (ODCs) (Travel, Materials, etc.)
- Funds Forecast (i.e. Spend Plans)
- Various Program Acquisition related documents: Mission Needs Statement (MNS), Capability Production Documentation (CPD), Operational
- Requirements Document (ORD), etc.
- Weekly reports on RMF status for system/enclave(s) (CDRL T002)
- Travel and leave tracker (CDRL T003)
- Cost estimate for system/enclave (CDRL T004)
- Available budget and expensed funding at system/enclave level (CDRL T005)

3.3 SECURITY CONTROLS ASSESSOR/REPRESENTATIVE (SCA/(R)) SUPPORT

3.3.1 The contractor shall provide subject matter expertise to develop and review plan to assess the security controls.

3.3.2 The contractor shall assess the security controls in accordance with the assessment procedures defined in the DHA security assessment plan.

3.3.3 The contractor shall prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment (SCA).

3.3.4 The contractor shall conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s) as appropriate.

3.3.5 The contractor shall assess a selected subset of the technical, management, and operational security controls employed within and inherited by information systems in accordance with the organization defined monitoring strategy.

3.4 ASSESMENT AND AUTHORIZATION (A&A) OF DHA INFORMATION TECHNOLOGY (IT) SUPPORT

-

3.4.1 The contractor shall support the DHA IT compliance with DoD IA RMF Directives and Processes by:

- Providing assistance to system owner, enclave, or site personnel to complete required RMF documentation;

- Addressing Independent Validation and Verification (IV&V) results and assisting enclave personnel in preparing all aspects of an Enterprise Mission Assurance Support Service (eMASS) authorization package for review by the Validator, Security Control Assessor/Representative (SCA(R)), or the Authorizing Official (AO);

- Reviewing Security Design documentation to ensure comprehensive security requirements and compliance with DoD and Federal requirements and guidelines;

- Reviewing and providing input on physical, application, and networking security policies, procedures, and practices;

- Updating any A&A Standard Operating Procedures (SOP) so that it aligns to DHA policies;

- Providing documentation support in the form of assisting with the writing and production of SOPs and Operational Manuals, and reviewing government established and created Policies and Procedures;

- Supporting the implementation of Federal IT Security regulations, directives and guidance (Federal Information Security Management Act - FISMA, Federal Information Processing Standard - FIPS, National Institute of Standards and Technology - NIST series);

- Documenting the IA test plan and procedures templates for inclusion in the Test Plan to appropriately relate the testing standard identified by the AO and SCA(R) activities.

3.4.2 The contractor shall support A&A Program Efforts with stakeholders by:

- Reviewing updates of the RMF artifacts from the system owner and tracking status of changes;

- Assisting in the development of the path to complete authorization;

- Assembling the RMF Package, (RMF Scorecard, POA&M, assessment documentation, and RMF System Implementation Plans (SIPs);

- Delivering the RMF Package to the SCA(R) in a trusted manner consistent with DHA and/or Program requirements;

- Providing A&A support in the areas of network topologies, file/application servers, encryption technologies, and network operating hardware and software

- Assessing the eMASS packages/POA&M scheduling and completeness status and report;

- Tracking assigned system from initiation to retirement while staying informed of IV&V milestones and RMF POA&M deadlines;

- Addressing authorization questions from the Program Management Office (PMO);

- Maintaining authorization schedules for systems and working with the PMO to ensure the correct A&A process is being followed;

- Adhering to all authorization guidance received from the SCA(R) and performing actions necessary to complete assessment;

- Participating in all test execution and planning activities, including meetings and working groups;

- Participating in RMF Team Meetings and System review related meetings and providing technical and non-technical guidance;

- Identifying and elevating the need for any additional IA test events needed to support authorization (includes scheduling of annual reviews)

3.4.3 The contractor shall support the DHA Cybersecurity Validation Readiness review efforts for both sites/enclaves and programs of records by:

- Reviewing the RMF IV&V Self-Assessment results;

- Evaluating the self-assessment results and evidence during Readiness Review to determine if the security is sufficiently mature to execute an assessment test event;

- Determining the IV&V test level of effort for each planned system or enclave;

- Participating in all test execution and planning activities, including meetings and working groups;

- Reviewing the RMF documentation prior to IV&V to determine security readiness of system, site, or enclave

3.4.4 The contractor shall support all of the necessary DHA RMF Independent Verification and Validation events assigned by:

- Supporting the IV&V testing of each system, site, or enclave under the SCA(R) and AO purview;

- Participating in all test execution and planning activities, including meetings and working groups and provide all minutes and meeting notes IAW DHA RMF process documents (CDRL T006);

- Reviewing all RMF documentation to ensure the information is current, accurate, and applicable to the article of test;

- Supporting standardization, by ensuring that all IA test procedures are up to date with all current applicable requirements and that those methods of testing are widely visible and available for DHA to apply to all necessary systems across its enterprise;

- Producing all necessary RMF security controls test procedures for inclusion in the Test Plan that describe how to perform validation actions as outlined in the applicable Security Technical Implementation Guide (STIG) checklists;

- Analyzing previous IA testing artifacts to ensure proper tailoring of IA tests is considered and accounted for;

- Developing the Security Assessment Plan (SAP), providing to the system owner, documentation team, and A&A team (CDRL T007)

- Overseeing the execution of testing to identify all vulnerabilities, and documenting all residual risks by conducting thorough risk assessments;

- Providing the IA risk analysis and mitigation determination results for use in the test report;

- Developing and/or utilizing automated tools, for the creation of necessary test evidence, risk assessment, and authorization artifacts for each system;

- Performing wireless discovery using DoD approved software;

- Performing all testing with tools capable of managing the test procedures and results;

- Providing appropriately qualified validator and IV&V representatives to review all RMF documentation prior to IV&V;

- Scheduling the IV&V test events and assigning IV&V team members to meet the requirements of the IV&V test plan;

- Providing all necessary status report to the Government PM to document the progress/results of IA testing in accordance with requirements established in the IV&V level of effort determination. (CDRL T008)

- Coordinating the test planning with Subject Matter Experts (SMEs) identified from IA Validation Team with the SCA(R)

3.4.5 The contractor shall provide oversight and support of the POA&M and RMF Scorecard creation by:

- Overseeing the completion of the RMF Scorecard within eMASS;

- Providing any Government approved mitigation and remediation in support of the RMF process both remotely and on-site (CDRL T009);

- Providing POA&M resolution recommendations to reduce residual risk in accordance with applicable DoD and Federal technical and operational requirements and guidelines (CDRL T010);

- Providing assistance to sites to update outstanding actions contained in the POA&M and assisting with the request of extensions for expiring ATOs or POA&M items;

3.4.6 The contractor shall provide formal RMF validation services of all submitted RMF packages within the DHA eMASS instance by:

- Maintaining any qualified validator status, in accordance with applicable DHA agency requirements;

- Reviewing all packages for accuracy and completeness before being delivered to SCA(R) and producing a package completeness report. (CDRLT011);

- Working directly with the SCA(R) as a qualified agent to ensure validation activities are compliant with the IA test strategy;

- Conducting in-depth analysis of IV&V, A&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal IA technical and operational security requirements;

- Working with the system owner or program manager to develop specific site or system mitigation plans to achieve an overall reduction in residual risk;

- Coordinating with the SCA(R) and providing consult for the issuance of a proper authorization recommendation that complies with all applicable DoD and Federal guidance.

3.4.7 The contractor shall provide support in performing proper risk assessments in accordance will all applicable DHA, DoD and Federal

requirements by:

- Conducting in-depth analysis of IV&V, A&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal IA technical and operational security requirements;

- Documenting residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth and providing the IA risk analysis and mitigation determination results for any required test or risk reports;

- Assisting the SCA(R) and/or Validator with producing the risk assessment artifacts describing residual risks identified during testing or analysis (CDRL T011)

3.5 CYBERSECURITY TOOL/TOOLSET ENHANCEMENT AND MAINTENANCE

3.5.1 The contractor shall provide appropriate program workflow experts and web developers to support the enhancement and maintenance of DHAs SharePoint enabled web based solution for a community-wide data collection and management system whose primary function is to:

- Expedite and streamline the process of tracking and reporting systems to DHA Leadership, A&A Users, System Owners and PMOs;

- Provide DHA Rollup Dashboard functionality to display system and authorization metrics from each underlying service;

- Provide Service level dashboards with filtered reports for each service;

- Increase visibility to the PMOs and System owners for their systems;

- Support managing the A&A processes across services;

- Track process steps (RMF and other applicable processes);

- Provide centralized portal for stakeholders to submit system/enclave associated issues and notes.

3.5.2 The contractor shall provide appropriately skilled application programming experts to support the enhancement and maintenance of DHA'S cybersecurity tool/toolset (including DISA provided tools) used in the assessment and authorization process. This tool/tools currently/should maintain the ability to streamline testing events within the DHA programs and enclaves by supporting the following non-exclusive requirement while maintaining 100% accuracy and transparency:

- Analyze raw ACAS results and automatically produce a report;

- Automation of inventories and providing a detailed, error-free report;

- Automation, identification and assignment of IV&V STIGs – identifies what's required and auto assigns STIGs to relevant host, creates a test plan, applies sampling guidance and creates fully random sample groups;

- Creates detailed vulnerability report;

- Lists all open ports on each host, ID's firewall/IDS interference, maintains plugin version control, and identifies targeted IP ranges;

- Automate the assessment and consolidation of security scans of systems;

- Improve accuracy of assessment with a goal of 100% accuracy;

- Be easily executed and highly collaborative;

- Reduce security overhead lowering IT lifecycle costs

3.5.3 The contractor shall provide appropriately skilled application programming experts to support the enhancement and maintenance of DHA'S cybersecurity tool/toolset for the DHA used in the assessment and authorization process. This tool/tools currently/should maintain the ability to streamline testing events within the DHA programs and enclaves by supporting the following non-exclusive requirements, while maintaining 100% accuracy and transparency:

- Ability to apply selected security controls, overlays, and Control Correlation Identifier (CCI's) to later technical STIG selection to de-conflict N/A assessment procedures;

- Provides extensive search capabilities to research specific CCIs or STIGs, general analyst inquiries, applicability research, etc.;

- Ability to provide for the bulk exchange of asset, checklist, and assessment information (evidence, comments, status) between SCA, PMO, and other relevant parties (vendors or commercial contractors);

- Ability to create a Security Assessment Plan (SAP) or test matrix from imported and manually generated data;

- Support the manual manipulation of assets and scan results to facilitate SAP build (ex: assign checklists to assets, de-conflict CCIs and N/A IA Controls, etc);

- Ability to produce a level-of-effort estimate for a testing event, including number of personnel, length of test event and cost associated with test event. (CDRL T001);

- Support intelligent automatic assignment of STIGs or security checklists using assigned meta data and Common Platform Enumeration (CPE) information;

- Support creation of default evidence, comments, and statuses for particular CCIs and rules to facilitate a speedy assessment;

- Support integration with other automated tools and data formats to expedite accurate assessments by importing common DoD and industry standards, mapping and de-conflicting rules between automated scans and supporting future integration of changing standards (and backwards compatibility);

- Export raw evidence data in industry formats (ex: MITRE Extensible Configuration Checklist Description Format (XCCDF) or DoD CKL) and eMASS ready and customizable POAMs

3.6 PROGRAM OFFICE RMF SUPPORT

3.6.1 The contractor shall provide RFM Documentation Support:

- Develop all RMF documentation in accordance with DoD/DHA policies and procedures to ensure that authorization packages are complete and system compliance accurately documented for the Authorizing Official (AO);

- Maintain documentation Plan of Action and Milestones;

- Work with the Program Management Office (PMO) to ensure that the correct RMF Process is being followed and participate in any required team meetings;

- Address authorization documentation questions from the PMO;

- Develop RMF documentation to ensure the information is current, accurate, and applicable to the article of test;

- Develop Cybersecurity self-assessment results and evidence during any Cybersecurity validation readiness reviews to determine if the system security is sufficiently mature to execute the Cybersecurity test event;

- Utilize Enterprise Mission Assurance Support Services (eMASS) and systems such as Continuous Monitoring and Risk Scoring (CMRS) for the documentation of test evidence and risk assessment for each system;

- Develop associated Cybersecurity artifacts to include, but not limited to, the System Security Plan, System Design and Architecture, Contingency Plan/Continuity of Operations Plan (COOP) Plan, Incident response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote artifacts;

- Provide all necessary status report to the Government PM documenting the progress/results of Program Office RMF Support (CDRL T012)

3.6.2 The contractor shall provide Self-Assessment Support:

- Work with Independent Verification & Validation (IV&V) Lead from DHA to develop test plans and participate in system related team meetings;

- Prepare for on-site self-assessments;

- Execute tests in accordance with test plans;

- Prepare test events status reports and out-briefs;

- Populate Validator databases such as eMASS and CMRS with test results and provide input into test event reporting;

- Assemble Cybersecurity package [e.g. Scorecard, Plans of Action & Milestones (POA&M), Certification Documentation, Implementation Plans];

- Develop plans to validate actions as outlined in the Security Technical Implementation Guide (STIG) checklists;

- Assist Cybersecurity/Information Assurance (IA) Analyst / Test Team Lead with evaluation Cybersecurity self-assessment results and evidence;

- Ensure Cybersecurity test procedures are available and visible for replication use across systems utilizing the same hardware and software;

- Utilize eMASS and the Defense Information System Agency’s (DISA) latest vulnerability management system for the documentation of test evidence and risk assessment for each system

3.7 TECHNICAL SUPPORT

3.7.1 Cybersecurity Documentation and Reports

The contractor shall be able to apply the Cybersecurity disciplines required to ensure that the technical support community is provided with adequate instruction including applied exercises resulting in the attainment and retention of knowledge, skills, attitudes, and subject matter expertise regarding applicable Cybersecurity systems. Contractor shall develop presentations, reports, white papers and training documentation as required.

4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

The contractor shall be responsible for the following:

4.1.1 Ensure that no production systems are operational on any research, development, test and evaluation (RDT&E) network.

4.1.2 Follow DoDI 8510.01 when deploying, integrating, and implementing IT capabilities.

4.1.3 Migrate all Navy Ashore production systems to the Navy, Marine Corps Intranet (NMCI) environment where available.

4.1.4 Work with Government personnel to ensure compliance with all current Navy IT & Cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

4.1.5 Follow SECNAVINST 5239.3B & DoDI 8510.01 prior to integration and implementation of IT solutions or systems.

4.1.6 Register any contractor-owned or contractor-maintained IT systems utilized on task order in the Department of Defense IT Portfolio Registry (DITPR)-DON.

4.1.7 Ensure all software recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, 26 CFR Part 1194 and pursuant to SPAWARINST 5721.1B.

4.1.8 Only perform work specified within the limitations of the basic contract and task order.

4.2 ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES

Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

4.2.1 DoN Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA), contractors that are authorized to use Government supply sources per FAR Subpart 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program as prescribed in DFARS Subpart 208.74 and Government-wide SmartBuy program (see DoD memo dtd 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. The contractor shall purchase the following software and/or software licenses:

Item #	Description, Estimated Base Year	Unit/Issue	Quantity
1	Adobe Pro	each	10
2	Microsoft Visio	each	10

Item #	Description, Estimated Option 1 Year	Unit/Issue	Quantity
1	Adobe Pro	each	10
2	Microsoft Visio	each	10

Item #	Description,Estimated Option 2 Year	Unit/Issue	Quantity
1	Adobe Pro	each	10
2	Microsoft Visio	each	10
Item #	**Description,Estimated Option 3 Year**	**Unit/Issue**	**Quantity**
1	Adobe Pro	each	10
2	Microsoft Visio	each	10

4.2.2 DoN Application and Database Management System (DADMS)

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

4.2.3 Cybersecurity/Computer Security Requirements

The contractor shall ensure that all products recommended and/or procured that impact Cybersecurity or Information Assurance (IA) shall be selected from the National Information Assurance Partnership (NIAP) Validated Products List. The contractor shall ensure the products chosen are based on the appropriate Evaluated Assurance Level (EAL) for the network involved, and are utilized in accordance with latest Defense Information Systems Agency (DISA) policy at time of order. The contractor shall store all product information and have it available for government review at any time.

4.3 SECURITY IT POSITION CATEGORIES

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R (and subsequent revisions), SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The contractor PM shall assist the Government Project Manager or Contracting Officer's representative (COR) in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. Requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access are submitted by NIWC Atlantic Security Office, processed by the OPM, and adjudicated by Department of Defense Consolidated Adjudications Facility (DoD CAF). IT Position Categories are determined based on the following criteria:

4.3.1 IT-I Level (Privileged)

Personnel in this position support Cybersecurity roles at command enclave infrastructure to include RDT&E, Data Centers and any other network and/or are responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation shall have a favorably adjudicated Tier 5 (T5) investigation (formerly a Single Scope Background Investigation (SSBI) or SSBI-PR). The T5 is updated a minimum of every 5 years. Personnel assigned to designated IT-I positions shall have a U.S. citizenship unless a waiver request is approved by CNO. IT-1 roles include the following:

- Boundary Devices Management (proxies, firewalls, traffic analyzers, VPN Gateways)
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Host Based Security Systems (HBSS)
- Network infrastructure (routers, switches, enterprise wireless)
- Domain and Authentication System Administrators (Active Directory, LDAP, Kerberos, etc.) (enclave wide scope)
- Vulnerability Scanner Operators (Retina, ACAS, HP Web Inspect, etc.)
- Virtualization Technology Administrators that host any of the above (ESX, Solaris Zones, etc.)

4.3.2 IT-II Level (Limited Privileged)

Personnel in this position support the-direction, planning, design, operation, or maintenance of a computer system, have privileged access to assets and systems that are tenants on NIWC Atlantic networks and/or similar system constructs, and has work that is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position shall have a favorably adjudicated Tier 3 (T3) investigation (formerly National Agency Check with Law and Credit (formerly ANACI/NACLC). Personnel assigned to designated IT-II positions shall have a U.S. citizenship unless a waiver request is approved by CNO. Examples of IT-II roles include the following:

- Webserver Administrators
- Developers
- Testers
- Database Administrators

4.3.3 IT-III Level (Non-privileged)

Personnel in this position support include all other positions (not considered IT-I or IT-II) involved in computer activities. A contractor in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation shall have a favorably adjudicated Tier 1 (T1) investigation National Agency Check with Written Inquiries (formerly NACI).

4.4 CYBERSECURITY SUPPORT

Cybersecurity (which replaced the term Information Assurance (IA) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy Cybersecurity requirements.

4.4.1 Cyber IT and Cybersecurity Personnel

4.4.1.1 The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing Cybersecurity functions shall meet all Cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M and subsequent manual [DoD 8140] when applicable prior to accessing DoD information systems. Proposed contractor Cyber IT and Cybersecurity personnel shall be appropriately qualified prior to the start of the task order performance period or before assignment to the task order during the course of the performance period.

4.4.1.2 Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in Para 8.2.2.4(b).

4.4.1.3 Contractor personnel with privileged access shall acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

4.4.2 Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the Cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management

System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in Para 4.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

4.4.3 Cybersecurity Workforce (CSWF) Report

In accordance with DFARS clause 252.239-7001 and DoD 8570.01-M, the contractor shall identify Cybersecurity personnel, also known as CSWF and Cyber IT workforce personnel. The contractor shall develop, maintain, and submit a monthly CSWF Report (CDRL T016) identifying CSWF individuals who are IA trained and certified. Utilizing the format provided in CDRL T016 Attachment 1 of Exhibit A, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Although the minimum frequency of reporting is monthly, the COR can require additional updates at any time. Contractor shall verify with the COR or other Government representative the proper labor category CSWF designation and certification requirements. The primary point of contact (POC) for all related CSWF questions is the Command CSWF Program Manager (PM) in the office of the NIWC Atlantic Information Systems Security Manager (ISSM).

4.4.4 Cybersecurity Workforce (CSWF) Designation

CSWF contractor personnel shall perform Cybersecurity functions. In accordance with DoD 8570.01-M Information Assurance Workforce Improvement Program Manual, the CSWF is comprised of the following categories: IA Technical (IAT) and IA Management (IAM)); and specialties: Computer Network Defense Service Providers (CND-SPs) and IA System Architects and Engineers (IASAEs). Based on the IA function provided by the individual, an IA designator is assigned that references an IA category or specialty. The following Labor Categories shall meet the IA Designator, IA Level/Position, and have the estimated Primary/Additional/Embedded hours performing IA duties:

Labor Category	**Quantity Personnel**	**IA Designator (Note1)**	**IA Level/Position (Note2)**	**IA Duty Hours**		
				Primary (=25 hrs)	**Additional (15-24 hrs)**	**Embedded (1-14 hrs)**
Engineer/Scientist 2	9	IAT	Level 2	X		
Engineer/Scientist 3	66	IAM	Level 1	X		
Engineer/Scientist 4	38	IAM	Level 2	X		
Engineer/Scientist 5	21	IAM	Level 3	X		
Technical Writer/Editor 2	2	IAT	Level 1	X		
Technical Writer/Editor 3	2	IAT	Level 1	X		
SME 2	14	IAT	Level 2	X		
SME 3	68	IAM	Level 1	X		
SME 4	50	IAM	Level 2	X		
SME 5	17	IAM	Level 3	X		
Project Manager	1	IAM	Level 3	X		

5.0 TASK ORDER ADMINISTRATION

Administration of the work being performed is required; it provides the Government a means for task order management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the Government’s requirements are met, delivered on schedule, and performed within budget.

5.1 CONTRACTING OFFICER’S REPRESENTATIVE (COR) DESIGNATION

The COR for this task order isidentified in Section G.

5.2 CONTRACTOR LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government Contracting Officer and COR. The contractor PM, located in the contractor's facility, shall ultimately be responsible for ensuring that the contractor's performance meets all Government contracting requirements within cost and schedule. PM shall have the requisite authority for full control over all company resources necessary for task order performance and be available to support emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate periodic meetings with the COR.

5.3 CONTRACTOR MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day including business and non-business hours in order to facilitate a timely task order response or modification in particular during urgent requirements.

5.3.1 Task order Administration & Documentation

Various types of administration documents are required throughout the life of the task order. At a minimum, the contractor shall provide the following documentation:

5.3.1.1 Task Order Status Report (TOSR)

The contractor shall develop Task Order Status Reports (CDRL T017) and submit it monthly, weekly, and/or as cited in the requirements of this task order. The prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor reports. The TOSR include the following variations of reports:

(a) Monthly TOSR – the contractor shall develop and submit a task order status report monthly at least 30 days after task order award on the 10th of each month for those months the task order is active. The contractor shall report on various task order functions: performance, schedule, financial, business relations, and staffing plan/key personnel; see applicable DD Form 1423 for additional reporting details and distribution instructions. This CDRL includes a Staffing Plan (CDRL T017 Attachment 1 of Exhibit A), Personnel Listing (CDRL T017 Attachment 2 of Exhibit A), and Government-furnished property (GFP) Template (CDRL T017 Attachment 3 of Exhibit A) necessary for additional data collection as applicable.

(b) Weekly TOSR – the contractor shall develop and submit a weekly status report which is e-mailed to the COR no later than close of business (COB) every Friday. The first report is required on the first Friday following the first full week after the task order award date. The contractor shall ensure the initial report includes a projected Plan Of Action and Milestones (POA&M). In lieu of a formal weekly report, larger, more complex task orders require an updated Earned Value Management report. At a minimum, the contractor shall include in the weekly report the following items and data:

1. Percentage of work completed

2. Percentage of funds expended per ship/sub/shore command and system

3. Updates to the POA&M and narratives to explain any variances

4. If applicable, notification when obligated costs have exceeded 75% of the amount authorized

(c) Data Calls – the contractor shall develop and submit a data call report which is e-mailed to the COR within six working hours of the request. The contractor shall ensure all information provided is the most current. Cost and funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum, the contractor shall include in the data call the following items and data:

1. Percentage of work completed

2. Percentage of funds expended

3. Updates to the POA&M and narratives to explain any variances

4. List of personnel (by location, security clearance, quantity)

5. Most current GFP and/or contractor acquired Property (CAP) listing

5.3.1.2 Task Order Closeout Report

The contractor shall develop a task order closeout report (CDRL T018) and submit it no later than 15 days before the task order completion date. The Prime shall be responsible for collecting, integrating, and reporting all subcontracting information. See applicable DD Form 1423 for additional reporting details and distribution instructions.

5.3.1.3 Enterprise-wide Contractor Manpower Reporting Application

Pursuant to NMCARS 5237.102-90, the contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this task order for the DoD via a secure data collection website – Enterprise-wide Contractor Manpower Reporting Application (eCMRA). The Product/Service Codes (PSC) for contracted services excluded from reporting are as follows:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) S, Utilities ONLY;

(5) V, Freight and Shipping ONLY.

The contractor shall completely fill-in all required data fields using the following web address: http:// ecmra.mil/. Reporting inputs consists of labor hours executed during the task order period of performance within each Government fiscal year (FY) which runs from October 1 through September 30. While inputs may be reported any time during the FY, the contractor shall report all data no later than October 31 of each calendar year. Contractors may direct questions to the help desk at http://www.ecmra.mil/.

5.3.1.4 WAWF Invoicing Notification and Support Documentation

Pursuant to DFARS clause 252.232-7003 and 252.232-7006, the contractor shall submit payment requests and receiving reports using DoD Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT) application (part of the Wide Area Work Flow (WAWF) e-Business Suite) which is a secure Government web-based system for electronic invoicing, receipt, and acceptance. The contractor shall provide e-mail notification to the COR when payment requests are submitted to the iRAPT/WAWF and the contractor shall include cost back–up documentation (e.g., delivery receipts, time sheets, & material/travel costs, etc.) to the invoice in iRAPT/WAWF. When requested by the COR, the contractor shall directly provide a soft copy of the invoice and any supporting invoice documentation (CDRL T019) directly to the COR within 24 hours of request to assist in validating the invoiced amount against the products/services provided during the billing cycle.

5.3.1.5 Labor Rate Limitation Notification

The contractor shall monitor labor rates as part of the monthly TOSR (see CDRL T017 Attachment 2 of Exhibit A – Personnel Listing). The contractor shall deliver required notification if specified criteria and threshold values are met. The ability of a contractor to monitor labor rates effectively will be included in the task order Quality Assurance Surveillance Plan (QASP).

(a) Fully burdened labor rates per individual (subcontractor included) – If the fully burdened rate (including fee, which also extends to prime contractor fee on subcontractor labor) of any individual in any labor category exceeds the threshold amount of $200.00/hour and the individual's rate was not disclosed in pre-award of the task order, the contractor shall send notice and rationale (CDRL T020) for the identified labor rate to the COR who will then send appropriate notification to the Contracting Officer. If the number of hours anticipated to be billed for an *individual* within one labor category is equal to or less than 200 labor hours for any given period of performance (e.g., base period, option year 1, or option year 2) for this effort, the hours to be billed for the individual are excluded from the CDRL notification.

(b) Negotiated versus actual average labor rates variance – If the actual average labor rate (inclusive of fee) (total actual fully burdened labor costs "divided by" total number of hours performed) is greater than 20% of the negotiated average labor rate (total negotiated fully burdened labor costs "divided by" total number of hours negotiated) , the contractor shall send notice and rationale (CDRL T020) of the rate variance to the COR who will then send appropriate notification to the Contracting Officer. The contractor shall annotate the monthly percentage rate variance between the actual average labor rate versus the negotiated average labor rate in the TOSR. If a negotiated versus actual average labor rate variance occurs only due to the specific composition of the monthly labor mix (rather than actual labor rates invoiced exceeding negotiated labor rates by greater than 20%), then the variance is excluded from the CDRL notification.

5.3.1.6 ODC Limitation Notification

Contractors shall monitor Other Direct Costs (ODCs) as part of the monthly TOSR. For this monitoring purpose, ODCs include incidental material, travel, and other non-labor costs (excluding subcontracting and consultant labor cost) required in performance of the service. For any given period of performance, if the cumulative total cost of ODCs exceeds the awarded total cost of ODCs (regardless of any modifications to the awarded amount) by 110% of the original ODC, the contractor shall send notice and rationale (CDRL T020) for exceeding cost to the COR who will then send a memorandum signed by the PM (or equivalent) to the Contracting Officer documenting the reasons justifying the increase of ODC. CDRL notification is not needed if the revised ODC total is below 10% of the total labor value or $3M, whichever is lower. The ability of a contractor to monitor ODCs will be included in the task order QASP.

5.4 CONTRACTOR PERFORMANCE MANAGEMENT

Contractor performance standards and requirements are outlined in the task order QASP. The ability of a contractor to perform to the outlined standards and requirement will be captured in the Contractor Performance Assessment Reporting System (CPARS). In support of tracking contractor performance, the contractor shall provide the following documents: Cost and Schedule Milestone Plan (CDRL T021) submitted 10 days after task order award and CPARS Draft Approval Document (CDAD) Report (CDRL T022) submitted monthly.

5.5 EARNED VALUE MANAGEMENT (EVM)

In accordance with DoD policy, this task order does not require Earned Value Management (EVM) implementation due to the majority of efforts on this task order is non-scheduled based (i.e., level of effort) and does not lend itself to meaningful EVM information. In lieu of an EVM system, the contractor shall develop and maintain, a Contract Funds Status Report (CDRL T023) to help track cost expenditures against performance.

-

6.0 DOCUMENTATION AND DELIVERABLES

6.1 CONTRACT DATA REQUIREMENTS LIST (CDRL)

The following listing identifies the data item deliverables required under this task order and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s that itemize each Contract Data Requirements List (CDRL) required under the basic contract. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task. The contractor shall not develop any CDRL classified TOP SECRET with SCI.

6.1.1 Administrative CDRL

The following table lists all required administrative data deliverables, CDRLs, applicable to this task:

CDRL #	Deliverable Title	PWS Reference Para
T016	Cybersecurity Workforce (CSWF) Report	4.4.3 8.1.2 8.2.3.1
T017	Task Order Status Report (TOSR)	5.3.1.1, 5.3.1.5, 8.1.2, 8.2.3.1, 10.2.1, 10.3.3.1,
T018	Task Order Closeout Report	5.3.1.2, 10.3.6
T019	Invoice Support Documentation	5.3.1.4
T020	Limitation Notification & Rationale	5.3.1.5, 5.3.1.6
T021	Cost and Milestones Schedule Plan	5.4
T022	Contractor CPARS Draft Approval Document (CDAD) Report	5.4
T023	Contract Funds Status Report (CFSR)*	5.5
T024	Quality Documentation	7.1, 7.4
T025	OCONUS Deployment Package	11.2.1

6.1.2 Technical CDRL

The following table lists all required technical data deliverables, (CDRLs), applicable to this task order:

T001	Program Management Reports	3.2.2, 3.5.3
T002	Weekly System Status Reports	3.2.2
T003	Travel and Leave Tracker	3.2.2
T004	Cost Estimate For System/Enclave	3.2.2
T005	Available Budget and Expensed Funding at System/Enclave Level	3.2.2
T006	Test Execution Planning Activities	3.4.4
T007	IV&V Test Plan	3.4.4
T008	Progress/Results Testing Report	3.4.4

T009	Mitigation and Remediation Support	3.4.5
T010	POA&M Resolution Recommendations	3.4.5
T011	Risk Assessment Artifacts	3.4.6, 3.4.7
T012	Program Office RMF Support Reports	3.6.1
T013	Inventory Tracking Report	10.2.1, 10.2.2.2, 10.3.3
T014	Warranty Tracking and Administration for Serialized Item Report	10.2.2.1 10.2.2.2
T015	Failure Status Repair Report	10.2.2.2

6.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the Government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, and etc., are provided in a format approved by the receiving Government representative. The contractor shall provide all data in an editable format compatible with NIWC Atlantic corporate standard software configuration as specified below. Contractor shall conform to NIWC Atlantic corporate standards within 30 days of task order award. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government.*

	Deliverable	**Software to be used**
a.	Word Processing / Reports	Microsoft Word/Adobe PDF
b.	Technical Publishing	Microsoft Word/Adobe PDF
c.	Spreadsheets	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	Diagrams/Schematics (new data products)	Microsoft Visio
g.	Scheduling	Microsoft Project

6.3 INFORMATION SYSTEM

6.3.1 Electronic Communication

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The contractor shall be capable of Public Key Infrastructure (PKI) client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on task shall be accessible by e-mail through individual accounts during all hours.

6.3.2 Information Security

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on task. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the task order, and privileged task order information (e.g., program schedules and task order-related tracking).

6.3.2.1 Safeguards

The contractor shall protect Government information and shall provide compliance documentation validating they are meeting this requirement in accordance with DFARS clause-252.204-7012. The contractor and all subcontractors shall abide by the following safeguards:

(a) Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

(b) Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

(c) Sanitize media (e.g., overwrite) before external release or disposal.

(d) Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. NOTE: Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, “Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage.” The contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.

(e) Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

(f) Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.

(g) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

(h) Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

(i) Provide protection against computer network intrusions and data exfiltration, minimally including the following:

1. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

2. Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

3. Prompt application of security-relevant software patches, service packs, and hot fixes.

(j) As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

(k) Report loss or unauthorized disclosure of information in accordance with contract, task order, or agreement requirements and mechanisms.

6.3.2.2 Compliance

Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements.

7.0 QUALITY

7.1 QUALITY SYSTEM

Upon task order award, the prime contractor shall have and maintain a quality system that meets contract and task order requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The contractor shall have an adequately documented quality system which contains processes, procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system, which includes an internal auditing system. Thirty (30) days after task order award, the contractor shall be able to provide, as requested by the Government, a copy of the contractor's Quality Assurance Plan (QAP) and any other quality related documents (CDRL T024). The contractor shall make their quality system available to the Government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this task order may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan or quality system, and development of quality related documents. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

- Establish documented, capable, and repeatable processes
- Track issues and associated changes needed
- Monitor and control critical process, product, and service variations
- Establish mechanisms for feedback of field product and service performance
- Implement and effective root-cause analysis and corrective action system
- Establish methods and procedures and create data used for continuous process improvement

7.2 MANAGE QUALITY COMPLIANCE

7.2.1 General

The contractor shall have processes in place that coincide with the government's quality management processes. The contractor shall use best industry practices including, when applicable, ISO/IEC 15288 for System life cycle processes and ISO/IEC 12207 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in event-driven milestones and reviews as stated in the Defense Acquisition University's (DAU's) DoD Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System Chart which is incorporates multiple DoD directives and instructions – specifically DoDD 5000.01 and DoDI 5000.02. The contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment of Lean Six Sigma methodologies in compliance with NIWC Atlantic requirements and with the SSC Engineering Process Office (EPO) Capability Maturity Model Integration (CMMI) program. As part of a team, the contractor shall support projects at NIWC Atlantic that are currently, or in the process of, being assessed under the SSC EPO CMMI program. The contractor shall be required to utilize the processes and procedures already established for the project and the SSC EPO CMMI program and deliver products that are compliant with the aforementioned processes and procedures. Although having a formal CMMI appraisal is desired, it is not required.

7.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified in the contractor's Quality Assurance Plan (QAP) or by the respective WBS, POA&M, or quality system/QMS documentation in support of continuous improvement. The contractor shall deliver related QAP and any associated procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes, products, and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related products, services, documents, and material in a category when noncompliance is established.

-

7.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified in the contractor QAP or by the respective WBS, POA&M, or quality system/QMS documentation. The contractor shall submit the following related quality objective evidence (CDRL T024) upon request:

- Detailed incoming receipt inspection records
- First article inspection records
- Certificates of Conformance
- Detailed sampling inspection records based upon MIL-STD-1916 (Verification Level III)
- Quality Measurement and Analysis metrics/data

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

As specified in the DoD Contract Security Classification Specification, DD Form 254, the contractor shall perform classified work under this task order. At time of task order award, the contractor shall have a SECRET facility clearance (FCL).

8.1.1.1 U.S. Government security clearance eligibility is required in order to access and handle classified and certain controlled unclassified information (CUI) while performing Security Control Assessor Support, Assessment & Authorizations, Cybersecurity Tool Enhancement and Maintenance, and Cybersecurity Documentation and Reports. The contractor shall not generate any SCI deliverables.

8.1.1.2 This task order allows for various levels of security to support specific PWS tasks. The following table outlines the minimum required security clearance per task. The contractor shall provide personnel meeting the specific minimum personnel clearance (PCL) to support the PWS tasks listed below

Required Security Clearance	**PWS Task Paragraph**
Secret	3.2 3.3, 3.4, 3.5, 3.6, and 3.7.
None required	All other PWS Task Paragraphs

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring clearance and/or access to Government facility/installation and/or access to information technology systems under this task order. The FSO is typically key management personnel who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this/task order. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on task order. Responsibilities include tracking all personnel assigned Government badges and entering/maintaining personnel security mandatory training information within the Staffing Plan document, which is an attachment to the task order status report (TOSR) (CDRL T017) and if applicable, updating and tracking data in the CSWF Report (CDRL T016)

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAV M-5510.30, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on this task order, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order, and if applicable, are certified/credentialed for the CSWF. A favorable background determination is determined by either a Tier 1 (T1) investigation, Tier 3 (T3) investigation, or Tier 5 (T5) investigation and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or NIWC Atlantic information. *Cost to meet these security requirements is not directly chargeable to task order.*

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum security requirements, the contractor shall permanently remove the individual from NIWC Atlantic facilities, projects, and/or programs. If an individual who has been submitted for a fitness determination or security clearance is "denied," receives an "Interim Declination," or unfavorable fingerprint, the contractor shall remove the individual from NIWC Atlantic facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task orders.

8.2.1 Personnel Clearance

The majority of personnel associated with this task order shall possess a SECRETpersonnel security clearance (PCL). These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the DoD CAF and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Any future revision to the respective directive and instruction will be applied as a task order modification. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense, Navy, and NIWC Atlantic security regulations. The contractor shall immediately report any security violation to the NIWC Atlantic Security Management Office, the COR, and Government Project Manager.

8.2.1.1 The following labor categories shall meet the required minimum personnel clearances (PCL):

Labor Category	**Required Minimum Personnel Security Clearance (PCL)**
Program Manager	Secret
Project Manager	Secret
Technical Writer/Editor 2	Secret
Technical Writer/Editor 3	Secret
Management Analyst 3	None required
Engineer/Scientist 2	Secret
Engineer/Scientist 3	Secret
Engineer/Scientist 4	Secret
Engineer/Scientist 5	Secret
Subject Matter Expert (SME) 2	Secret
Subject Matter Expert (SME) 3	Secret
Subject Matter Expert (SME) 4	Secret
Subject Matter Expert (SME) 5	Secret

8.2.2 Access Control of Contractor Personnel

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) The majority of Government facilities require contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. For admission to NIWC Atlantic facilities/installations, the contractor shall forward a visit request to Joint Personnel Adjudication System (JPAS) /SMO 652366, or submit request on company or agency letterhead by fax to (843)218-4045 or mail to Space and Naval Warfare Systems Center Atlantic, P.O. Box 190022, North Charleston, SC 29419-9022, Attn: Security Office. For visitation to all other Government locations, the contractor shall forward visit request documentation directly to the on-site facility/installation security office.

(b) Depending on the facility/installation regulations, contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement. NOTE: NIWC Atlantic facilities located on Joint Base Charleston require a Common Access Card (CAC) each time physical installation access is required. Contractor shall contact NIWC Atlantic Security Office directly for latest policy.

(c) All contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location.

8.2.2.2 Identification and Disclosure Requirements

Contractor and subcontractor employees shall take all means necessary to not represent themselves as Government employees. All contractor personnel shall follow the identification and Government facility disclosure requirement as specified in Section H, Contractor Identification.

8.2.2.3 Government Badge Requirements

Some contract personnel shall require a Government issued picture badge in accordance with Section H, Contractor Picture Badge. While on Government installations/facilities, contractors shall abide by each site's security badge requirements. Various Government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF-86 for CAC) to the applicable Government security office via the COR. The contractor FSO shall track all personnel holding local Government badges at the task order level.

8.2.2.4 Common Access Card (CAC) Requirements

Some Government facilities/installations (e.g., Joint Base Charleston) require contractor personnel to have a CAC for physical access to the facilities or installations. Contractors supporting work that requires access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

(a) Pursuant to DoDM 1000.13-V1, issuance of a CAC is based on the following four criteria:

1. eligibility for a CAC – to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD federally controlled facilities on behalf of the NIWC Atlanti on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site o remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.

2. verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibili Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS).

3. completion of background vetting requirements according to FIPS PUB 201-2 and DoD 5200.2-R – at a minimum, the completion of FBI fingerprint check with favorable results and submission of a T1 investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Contractor personnel requiring logical access shall obtain and maintain a favorable T3 investigation. Contractor personnel shall contact the NIWC Atlantic Security Office to obtain the latest CAC requirements and procedures.

4. verification of a claimed identity – all contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employme Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federa Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a PKI. A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the task order specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual Cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Atlantic Information Systems Security Management (ISSM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requirin initial training and do not have a CAC, contact the NIWC Atlantic ISSM office at phone number (843)218-6152 or e-mail questions to ssclant_itsecmgt.fct@navy.milfor additional instructions. Training can be taken at the IAM office or online at https://iase.disa.mil/Pages/index.aspx.

2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NIWC Atlantic ISSM office or from the website: https://navalforms.documentservices.dla.mil/. Digitally signed forms will be routed to the ISSM office via encrypted e-mai to ssclant_itsecmgt.fct@navy.mil.

8.2.2.5 Contractor Check-in and Check-out Procedures

All NIWC Atlantic contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a NIWC Atlantic Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out Instruction and Forms as posted on the Command Operating Guide (COG) website. Throughout task order performance, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this task order within the required timeframe as cited in the Check-in and Check-out instructions. The contractor (FSO, if applicable) shall ensure all contractor employees whose services are no longer required on this task order return all applicable Government documents/badges to the appropriate Government representative. NOTE: If the contractor does not have access to the NIWC Atlantic COG website, the contractor shall get all necessary instruction and forms from the COR.

8.2.2.6 Accessing Navy Enterprise Resources Planning (ERP) System

Contractor personnel shall not access the Navy Enterprise Resource Planning (Navy ERP) system.

8.2.3 Security Training

Applicable for unclassified and classified contracts, contractor personnel (including subcontractors) shall complete all required mandatory Government training in accordance with COMSPAWARSYSCOM Code 80330 mandatory training webpage: https://wiki.spawar.navy.mil/confluence/display/HQ/Employee+Mandatory+Training. Contractors without access to the SPAWAR webpage shall coordinate with the COR concerning mandatory training as listed on the training webpage.

8.2.3.1 The contractor shall be responsible for verifying applicable personnel receive all required training. At a minimum, the contractor (FSO, if applicable) shall track the following information: security clearance information; dates possessing CACs; issuance and expiration dates for NIWC Atlantic badge; Cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training; CSWF certifications; etc. The contractor shall report individual contractor personnel training status by completing and updating the monthly task order status report (TOSR) Staffing Plan (CDRL T017) Attachment 1 of Exhibit A), Training tab. For Cybersecurity Workforce (CSWF) contractor personnel, all mandatory Cybersecurity training and certifications shall be reported in the CSWF Report (CDRL T016)

8.2.3.2 The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E and SPAWARINST 3432.1, NIWC Atlantic's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual and SPAWARSYSCENLANTINST 3070.1B. Note: OPSEC requirements are applicable when task order personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The contractor shall development their own internal OPSEC program specific to the task order and based on NIWC Atlantic OPSEC requirements. At a minimum, the contractor's program shall identify the current NIWC Atlantic site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training in accordance with requirements outline in the Security Training, Para 8.2.3. OPSEC training requirements are applicable for personnel during their entire term supporting this NIWC Atlantic task order.

8.3.3 NIWC Atlantic OPSEC Program

Contractor shall participate in NIWC Atlantic OPSEC program briefings and working meetings, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

OPSEC requirements identified under a classified contract shall have specific OPSEC requirements listed on the DD Form 254.

8.4 EFFECTIVE USE OF CONTROLS

The contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect task order related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure provisions are in place that will safeguard all aspects of information operations pertaining to this task order in compliance with all applicable PWS references. In compliance with Para 6.4.2.1, the contractor shall ensure Data-at-Rest is required on all portable electronic devices including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation. The contractor shall follow minimum standard in SECNAV M-5510-36 for classifying, safeguarding, transmitting, and destroying classified information.

9.0 GOVERNMENT FURNISHED INFORMATION (GFI)

Government Furnished Information (GFI) is Government owned intellectual property provided to contractors for performance on a task order. For the purposes of this task order, GFI includes manuals, technical specifications, maps, building designs, schedules, drawings, test data, etc. Depending on information contained in a document, the contractor shall comply with additional controls (e.g., completion of a Non-Disclosure Agreements, etc.) for access and distribution.

-

GFI is not anticipated on this task order.

10.0 GOVERNMENT PROPERTY

As defined in FAR Part 45, Government property is property owned or leased by the Government which includes Government-furnished property (GFP) and Contractor-acquired property (CAP). Government property is material, equipment, special tooling, special test equipment, and real property.

Government property includes both GFP and CAP, but does not include intellectual property and software. The contractor shall have established property management procedures and an appropriate property management point of contact who shall work with the assigned Government

Property Administrator to ensure their property management system is acceptable.

10.1 GOVERNMENT-FURNISHED PROPERTY (GFP)

As defined in FAR Part 45, GFP is property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. GFP includes spares and property furnished for repair, maintenance, overhaul, or modification. GFP includes Government-furnished equipment (GFE), Government-furnished material (GFM), Special Tooling (ST) and Special Test Equipment (STE).

-

GFP will not be provided on this task order.

10.2 CONTRACTOR-ACQUIRED PROPERTY (CAP)

As defined in FAR Part 45, CAP is property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title but has not yet performed receipt and acceptance. CAP consists of Contractor-acquired equipment (CAE), Contractor-acquired material (CAM), ST, and STE.

-

Pursuant to SPAWARINST 4440.12A, the contractor shall provide CAP identified in the table below. CAP items are acquired, fabricated, or otherwise providedby the contractor to support the task order and may be wholly provided to NIWC Atlantic, incorporated into a system, consumed, or delivered as an end item in the performance of the task order. Prior to actual items being acquired, fabricated, or otherwise provided, the contractor shall obtain COR concurrence.

Item #	Description, CAP - Estimated Base Year	Part #	Unit/Issue	Quantity
1	Laptops with a government provided Windows 10 computing platform image	E6520	EA	293
2	Miscellaneous Office Supplies	VARIOUS	LOT	1

Item #	Description, CAP - Estimated Option 1 Year	Part #	Unit/Issue	Quantity
1	Laptops with a government provided Windows 10 computing platform image	E6520	EA	100
2	Miscellaneous Office Supplies	VARIOUS	LOT	1

Item #	Description, CAP - Estimated Option 2 Year	Part #	Unit/Issue	Quantity
1	Laptops with a government provided Windows 10 computing platform image	E6520	EA	100
2	Miscellaneous Office Supplies	VARIOUS	LOT	1

Item #	Description, CAP - Estimated	Part #	Unit/Issue	Quantity

	Option 3 Year			
1	Laptops with a government provided Windows 10 computing platform image	E6520	EA	100
2	Miscellaneous Office Supplies	VARIOUS	LOT	1

10.2.1 Equipment and Material Procurement

The contractor shall research specified CAP as utilized within the task parameters. To ensure fair and reasonable pricing under this cost reimbursable line item, the contractor shall ensure acquisition selection factors include price, availability, reliability, and supportability within current supply system. The contractor shall keep source selection records and make it available for government review as needed. Prior to items being purchased, the contractor shall obtain COR concurrence. The contractor shall provide all support data and cost estimates necessary to justify a fair and reasonable price per item procured. The contractor shall have an adequate accounting system to track all items and the delivery status per task order and per item. After receipt, the contractor shall have an adequate property management system to track the item location per task order per item. All items procured by the contractor shall be utilized or staged at the contractor's facility transported by the contractor to the installation, integrated or consumed in a system, or returned to the government at the completion of the task order. The contractor shall be responsible for identifying monthly and cumulative CAP procurements in the TOSR (CDRL T017). At any time outside the monthly reporting cycle, the contractor shall be capable of generating a CAP inventory tracking report(s) (CDRL T013) of items procured, received, and delivered as applicable. Contractor shall recommend and procure items that conform to the following applicable product validation, identification, and tracking requirements.

10.2.1.1 Product Validation – The contractor shall certify that it purchases supplies from authorized resellers and/or distributers. The contractor shall warrant that the products are new, in their original box. The contractor shall obtain all manufacturer products submitted in task order offers from authentic manufacturers or through legal distribution channels only, in accordance with all applicable laws and policies at the time of purchase. The contractor shall provide the Government with a copy of the End User license agreement, and shall warrant that all manufacturer software is licensed originally to Government as the original licensee authorized to use the manufacturer software. The contractor shall track the licensing information and have it available for government review.

10.2.1.2 IT Security Requirements – The contractor shall ensure that all products recommended and/or procured meet Cybersecurity and computer requirements specified in PWS Para 4.0.

10.2.1.3 Electronic Parts – In order to mitigate use of counterfeit and/or defective electronic parts, the contractor shall ensure all acquired electronic parts comply with the notification, inspection, testing, and authentication requirements in accordance with DFARS clauses 252.246-7007 and DFARS clause 252.246-7008 specific to for electronic parts.

10.2.1.4 Item Unique Identification (IUID) – In accordance with SECNAVINST 4440.34, the contractor shall ensure that certain delivered items manufactured, integrated, or purchased (depending if item meets a unit cost threshold, is serially managed, or if government specifies identification required) have an item unique identification or Unique Item Identifier (UII). If specified by the Government, prior to delivery, the contractor shall clearly mark and identify each applicable item based on the guidance provided in DoD MIL-STD-130N for those items not already marked. With Government concurrence, the contractor shall specify the construct, syntax, marking methodology, and quality methodology chosen to mark the required parts and any corresponding technical justification. All IUID information shall be recorded and shall be subject to Government review. The contractor shall track IUID items and maintain information being recorded. Prior to delivery of applicable CAP item, the contractor shall register items with Unique Item Identifier (UII) in the IUID Registry.

10.2.2 Warranty Tracking & Management

10.2.2.1 Warranty Tracking Of Serialized Items

In accordance with DFARS clause 252.246-7005/7006 and Instructions for Electronic Submission of Warranty Tracking and Administration Information for Serialized Items (see CDRL T014 Attachment 1 of Exhibit A), the contractor shall follow the requirements for any serialized item manufactured or acquired that come with a warranty:

(a) For Government specified warranty terms – the Government will complete certain fields on the Warranty Tracking Information (WTI) form and Warranty Source of Repair Instructions (WSRI) form. The contractor shall complete the remaining sections of the WTI and forward the form as part of their task order proposal prior to award. The contractor shall complete the remaining sections of WSRI and forward the form (CDRL T014) to the Contracting Officer and COR at time of delivery of the warranted serialized item(s).

(b) For contractor/vendor specified warranty terms – the contractor shall complete all data elements for both the WTI and WSRI and shall forward the completed forms (CDRL T014) to the Contracting Officer and COR no later than the date the warranted serialized items are presented for receipt and/or acceptance.

(c) For receipt and acceptance of items – the contractor shall comply with the following requirements:

(i) Utilizing the Wide Area WorkFlow (WAWF), the contractor shall ensure that the required warranty data is electronically submitted using the CDRL exhibit line item number (ELIN) functionality for the WAWF Materiel Inspection and Receiving Report or WAWF Reparable Receiving Report, as applicable.

(ii) If problems occur submitting warranty data electronically, the WTI and WSRI can be submitted manually (as a PDF file) with the COR concurrence. The contractor shall forward documents to COR for review and when approved, the Government will post forms to Electronic Dat Access (EDA).

10.2.2.2 Warranty Management

The contractor shall serve as the warranty manager by tracking the applicable government acceptance dates/receipt dates against the serial number of equipment or the lowest replaceable unit (LRU) of a system. As warranty manager, the contractor shall, unless otherwise directed, submit warranty data on Warranty Tracking Information (WTI) form and Warranty Source of Repair Instructions (WSRI) as specified on the Warranty Tracking and Administration for Serialized Items (CDRL T014) The contractor shall upload data to the WAWF Materiel Inspection and Receiving Report (or WAWF Reparable Receiving Report, if appropriate).

(a) If no compatible Government database to maintain and track warranty life spans for the GFP and/or CAP under task order, the contractor shall internally track items by task order, serial numbers, and the information shall be updated monthly to identify the time left on the original warranty. The contractor shall provide the government a copy of the warranty information in an inventory tracking report (CDRL T013).

(b) When an item has failed, the contractor shall determine if the item is still under warranty. If the item is under warranty, the contractor shall obtain a Return for Maintenance Authorization (RMA) number and instructions on how to get the product repaired or replaced from the manufacturer or authorized distributor. A Warranty and Non-Warranty Failure Status Repair Report (CDRL T015) shall be submitted to the COR on all warranty and non-warranty actions taken during the preceding quarter and collected cumulatively. The contractor shall submit the report within fifteen (15) days of the completion of the quarter. Quarters will be based on the fiscal year beginning in the month of October.

10.3 GOVERNMENT PROPERTY MANAGEMENT

10.3.1 Contractor Property Management System

Pursuant to FAR clause 52.245-1 and DFARS clause 252.245-7003, the contractor shall establish and maintain an acceptable property management system that is subject to review and approval by the Contracting Officer and task order Government Property Administrator. The contractor's property management system shall adhere to the applicable prescribed requirements in FAR clause 52.245-1 and include the required data elements in DFARS clause 252.211-7007. The contractor shall ensure GFP in the possession of a subcontractor shall also be reported using the required data elements cited in DFARS clause 252.211-7007.

10.3.2 Government Property Administrator

As allowed by FAR Subpart 42.201, the contract property administrator under this contract is, unless otherwise designated, the Defense Contract Management Agency (DCMA). The contractor shall work with the Contracting Officer appointed PA to ensure compliance with the contract's property requirements in accordance with DoDI 4161.02 and the Guidebook for Contract Property Administration. For contractors without an approved property management system, the contractor shall contact the appointed PA within 30 days of contract award, and provide a copy of their property management procedures with the names of appropriate points of contact.

-

10.3.3 Government Property Records

Pursuant to FAR clause 52.245-1, contractors and any subcontractors if applicable shall be responsible for establishing and maintaining records of Government Property in their possession – this includes GFP and CAP. The contractor shall ensure GFP and CAP records contain, at a minimum, the data elements as described in FAR clause 52.245-1 and GFP records also contain the data elements specified in the DFARS clause 252.211-7007.

10.3.3.1 The contractor shall ensure all GFP and CAP identified in the Contractor's Property Management System are designated appropriately as material, equipment, ST and/or STE. The contractor shall work with the COR and designated contract Property Administrator to maintain adequate GFP records. The contractor shall forward the GFP inventory to NIWC Atlantic functional mailbox for review, tracking, and centralization which is required as part of the monthly TOSR (CDRL T017)

10.3.3 CAP Inventory and Warranty Tracking

The contractor shall create and maintain internal records of all Government property accountable to the task order, including GFP and CAP. In accordance with DFARS clause 252.246-7006, the contractor shall record each item delivered and/or ordered in a Material Inspection and Receiving Report/Inventory Tracking Report which are subject to review and delivery as requested (CDRL T013). At a minimum, the report shall track the following information: item description, order date, serial number, model number, lot number, delivery location, and the manufacturer warranty period and expiration date, if applicable. The contractor shall have inventory report information available for Government review, and the contractor shall ensure the report information has the ability to be sorted and manipulated by any of the input fields.

10.3.4 Government Property Transferring Accountability

GFP cannot be transferred between contracts or task orders unless approval is obtained from the Contracting Officer, proper identification/tracking is maintained, and modifications are issued to both affected contracts and/or task orders. Unlike GFP, CAP cannot be transferred. If CAP is required to be utilized on a contract or task order other than the one that funded its acquisition, it must be delivered to the Government. Once received and accepted by the Government, it can be provided as GFP on the same or another contract.

10.3.5 Government Property Lost or Damaged Items

Contractor shall promptly report to the COR and Contracting Officer all lost and/or damaged Government property. The requirements and procedures for reporting lost Government Property are specified in DFARS clause 252.245-7002.

10.3.6 Government Property Inventory Disposition

When disposition instructions for GFP are contained in the accountable task order or on the supporting shipping documents (DD Form 1149), the Contractor shall initiate and submit an excess inventory listing to the Contracting Officer, via the activity Property Administrator.

Pursuant to DFARS clause 252.245-7004, when disposition instructions are not stipulated in the task order or supporting shipping document (DD Form 1149), an excess inventory listing is required that identifies GFP and, under cost reimbursement contracts, CAP. The contractor shall submit the list to the COR and PCO, via the activity Property Administrator, at which time disposition instructions will be provided by the Government.

Note: If any Government property is slated for demilitarization, mutilation, or destruction by the contractor, the event shall be witnessed and verified by the COR or the designated Government personnel.

The contractor shall include a final inventory reporting list in the task order Closeout Report (CDRL T018). At the time of the contractor's regular annual inventory, the contractor shall provide the PCO, via the assigned Property Administrator, a copy of the physical inventory listing. All contractor personnel shall be responsible for following the company's internal inventory management procedures and correcting any problems noted by the Government Property Administrator.

10.3.7 Government Property Performance Evaluation

Non-compliance with Government Property terms and conditions will negatively affect the contractor's annual CPARS rating.

10.4 TRANSPORTATION OF EQUIPMENT/MATERIAL

Transportation of equipment and/or material is applicable for the noted GFP and/or CAP. This

requirement is for the base year and each option year. The contractor shall plan for the following transportation requirements which any shipping and shipping material consideration:

Type **(GFP/CAP)**	**Item Description**	**Qty**	**Origination**	**Destination**	**Schedule**	**Responsibility** **(GOVT/CTR)**
CAP	Laptop	5	Charleston, SC	Falls Church, VA	AS REQ	CTR
CAP	Laptop	5	Charleston, SC	San Antonio, TX	AS REQ	CTR

11.0 TRAVEL

11.1 LOCATIONS

The contractor shall be prepared to travel to the following locations. Prior to any travel taken in support of this task order, the contractor shall obtain COR concurrence. Travel to foreign countries outside of the continental United States (OCONUS) is required. The applicable countries include the following:Japan, Spain, Germany, Italy, and Indonesia. Prior to travel, the contractor shall meet all necessary travel requirements for their company and personnel to support work in the noted foreign OCONUS sites.

Base

# Trips	# People	# Days/Nights	From (Location)	To (Location)
38	22	5/4	Charleston, SC	Bethesda, MD
4	2	6/5	Charleston, SC	Guantanamo Bay
4	2	6/5	Charleston, SC	Yokosuka, Japan
4	2	5/4	Charleston, SC	Corpus Christi, TX

4	2	5/4	Charleston, SC	Portsmouth, VA
6	1	6/5	Charleston, SC	Rota, Spain
2	2	5/4	Charleston, SC	Fort Hood, TX
2	2	5/4	Charleston, SC	Fort Irwin, CA
2	2	5/4	Charleston, SC	Aberdeen, MD
2	2	5/4	Charleston, SC	Fort Meade, MD
2	2	5/4	Charleston, SC	Fort Jackson, SC
2	2	5/4	Charleston, SC	Fort Drum, NY
2	2	5/4	Charleston, SC	Fort Lee, VA
1	2	6/5	Charleston, SC	Jakarta, Indonesia
2	2	5/4	Charleston, SC	Fort Knox, KY
2	2	5/4	Charleston, SC	Carlisle Barracks, PA
2	2	6/5	Charleston, SC	Naples, Italy
2	2	5/4	Charleston, SC	Honolulu, HI
2	2	6/5	Charleston, SC	Sicily, Italy
2	2	5/4	Charleston, SC	Fort Rucker, AL
2	2	5/4	Charleston, SC	Fort Riley, KS
4	2	5/4	Charleston, SC	Fort Belvoir, VA
2	9	14/13	Charleston, SC	Portsmouth, VA
4	2	6/5	Charleston, SC	Stuttgart, Germany
2	2	5/4	Charleston, SC	Corpus Christi, TX
2	2	5/4	Charleston, SC	West Point, NY
2	2	5/4	Charleston, SC	Fort Eustis, VA
2	14	14/13	Charleston, SC	San Francisco, CA
4	2	5/4	Charleston, SC	Dulles, VA
4	4	10/9	Charleston, SC	NH Beaufort
2	2	5/4	Charleston, SC	Dayton, OH
2	4	5/4	Charleston, SC	Biloxi, MS
6	5	5/4	Charleston, SC	Bremerton, WA
2	5	5/4	Charleston, SC	Portsmouth, VA
2	4	6/5	Charleston, SC	Spokane, WA
2	6	5/4	Charleston, SC	San Diego, CA
2	6	5/4	Charleston, SC	Jacksonville, NC
1	5	11/10	Charleston, SC	United Kingdom

Option Year 1

# Trips	# People	# Days/Nights	From (Location)	To (Location)
38	22	5/4	Charleston, SC	Bethesda, MD
4	2	6/5	Charleston, SC	Guantanamo Bay
4	2	6/5	Charleston, SC	Yokosuka, Japan
4	2	5/4	Charleston, SC	Corpus Christi, TX
4	2	5/4	Charleston, SC	Portsmouth, VA
6	1	6/5	Charleston, SC	Rota, Spain
2	2	5/4	Charleston, SC	Fort Hood, TX
2	2	5/4	Charleston, SC	Fort Irwin, CA
2	2	5/4	Charleston, SC	Aberdeen, MD
2	2	5/4	Charleston, SC	Fort Meade, MD
2	2	5/4	Charleston, SC	Fort Jackson, SC
2	2	5/4	Charleston, SC	Fort Drum, NY
2	2	5/4	Charleston, SC	Fort Lee, VA
1	2	6/5	Charleston, SC	Jakarta, Indonesia
2	2	5/4	Charleston, SC	Fort Knox, KY
2	2	5/4	Charleston, SC	Carlisle Barracks, PA
2	2	6/5	Charleston, SC	Naples, Italy
2	2	5/4	Charleston, SC	Honolulu, HI
2	2	6/5	Charleston, SC	Sicily, Italy

2	2	5/4	Charleston, SC	Fort Rucker, AL
2	2	5/4	Charleston, SC	Fort Riley, KS
4	2	5/4	Charleston, SC	Fort Belvoir, VA
2	9	14/13	Charleston, SC	Portsmouth, VA
4	2	6/5	Charleston, SC	Stuttgart, Germany
2	2	5/4	Charleston, SC	Corpus Christi, TX
2	2	5/4	Charleston, SC	West Point, NY
2	2	5/4	Charleston, SC	Fort Eustis, VA
2	14	14/13	Charleston, SC	San Francisco, CA
4	2	5/4	Charleston, SC	Dulles, VA
4	4	10/9	Charleston, SC	NH Beaufort
2	2	5/4	Charleston, SC	Dayton, OH
2	4	5/4	Charleston, SC	Biloxi, MS
6	5	5/4	Charleston, SC	Bremerton, WA
2	5	5/4	Charleston, SC	Portsmouth, VA
2	4	6/5	Charleston, SC	Spokane, WA
2	6	5/4	Charleston, SC	San Diego, CA
2	6	5/4	Charleston, SC	Jacksonville, NC

Option Year 2

# Trips	# People	# Days/Nights	From (Location)	To (Location)
38	22	5/4	Charleston, SC	Bethesda, MD
4	2	6/5	Charleston, SC	Guantanamo Bay
4	2	6/5	Charleston, SC	Yokosuka, Japan
4	2	5/4	Charleston, SC	Corpus Christi, TX
4	2	5/4	Charleston, SC	Portsmouth, VA
6	1	6/5	Charleston, SC	Rota, Spain
2	2	5/4	Charleston, SC	Fort Hood, TX
2	2	5/4	Charleston, SC	Fort Irwin, CA
2	2	5/4	Charleston, SC	Aberdeen, MD
2	2	5/4	Charleston, SC	Fort Meade, MD
2	2	5/4	Charleston, SC	Fort Jackson, SC
2	2	5/4	Charleston, SC	Fort Drum, NY
2	2	5/4	Charleston, SC	Fort Lee, VA
1	2	6/5	Charleston, SC	Jakarta, Indonesia
2	2	5/4	Charleston, SC	Fort Knox, KY
2	2	5/4	Charleston, SC	Carlisle Barracks, PA
2	2	6/5	Charleston, SC	Naples, Italy
2	2	5/4	Charleston, SC	Honolulu, HI
2	2	6/5	Charleston, SC	Sicily, Italy
2	2	5/4	Charleston, SC	Fort Rucker, AL
2	2	5/4	Charleston, SC	Fort Riley, KS
4	2	5/4	Charleston, SC	Fort Belvoir, VA
2	9	14/13	Charleston, SC	Portsmouth, VA
4	2	6/5	Charleston, SC	Stuttgart, Germany
2	2	5/4	Charleston, SC	Corpus Christi, TX
2	2	5/4	Charleston, SC	West Point, NY
2	2	5/4	Charleston, SC	Fort Eustis, VA
2	14	14/13	Charleston, SC	San Francisco, CA
4	2	5/4	Charleston, SC	Dulles, VA
4	4	10/9	Charleston, SC	NH Beaufort
2	2	5/4	Charleston, SC	Dayton, OH
2	4	5/4	Charleston, SC	Biloxi, MS
6	5	5/4	Charleston, SC	Bremerton, WA

2	5	5/4	Charleston, SC	Portsmouth, VA
2	4	6/5	Charleston, SC	Spokane, WA
2	6	5/4	Charleston, SC	San Diego, CA
2	6	5/4	Charleston, SC	Jacksonville, NC

Option Year 3

# Trips	# People	# Days/Nights	From (Location)	To (Location)
38	22	5/4	Charleston, SC	Bethesda, MD
4	2	6/5	Charleston, SC	Guantanamo Bay
4	2	6/5	Charleston, SC	Yokosuka, Japan
4	2	5/4	Charleston, SC	Corpus Christi, TX
4	2	5/4	Charleston, SC	Portsmouth, VA
6	1	6/5	Charleston, SC	Rota, Spain
2	2	5/4	Charleston, SC	Fort Hood, TX
2	2	5/4	Charleston, SC	Fort Irwin, CA
2	2	5/4	Charleston, SC	Aberdeen, MD
2	2	5/4	Charleston, SC	Fort Meade, MD
2	2	5/4	Charleston, SC	Fort Jackson, SC
2	2	5/4	Charleston, SC	Fort Drum, NY
2	2	5/4	Charleston, SC	Fort Lee, VA
1	2	6/5	Charleston, SC	Jakarta, Indonesia
2	2	5/4	Charleston, SC	Fort Knox, KY
2	2	5/4	Charleston, SC	Carlisle Barracks, PA
2	2	6/5	Charleston, SC	Naples, Italy
2	2	5/4	Charleston, SC	Honolulu, HI
2	2	6/5	Charleston, SC	Sicily, Italy
2	2	5/4	Charleston, SC	Fort Rucker, AL
2	2	5/4	Charleston, SC	Fort Riley, KS
4	2	5/4	Charleston, SC	Fort Belvoir, VA
2	9	14/13	Charleston, SC	Portsmouth, VA
4	2	6/5	Charleston, SC	Stuttgart, Germany
2	2	5/4	Charleston, SC	Corpus Christi, TX
2	2	5/4	Charleston, SC	West Point, NY
2	2	5/4	Charleston, SC	Fort Eustis, VA
2	14	14/13	Charleston, SC	San Francisco, CA
4	2	5/4	Charleston, SC	Dulles, VA
4	4	10/9	Charleston, SC	NH Beaufort
2	2	5/4	Charleston, SC	Dayton, OH
2	4	5/4	Charleston, SC	Biloxi, MS
6	5	5/4	Charleston, SC	Bremerton, WA
2	5	5/4	Charleston, SC	Portsmouth, VA
2	4	6/5	Charleston, SC	Spokane, WA
2	6	5/4	Charleston, SC	San Diego, CA
2	6	5/4	Charleston, SC	Jacksonville, NC

11.2 OCONUS TRAVEL REQUIREMENTS

Pursuant to SPAWARSYSCENLANTINST 12910.1B, DoDI 3020.41, and the latest DoD Foreign Clearance Guide requirements, the contractor shall travel outside the continental United States (OCONUS) sites to support deployed forces.

11.2.1 General OCONUS Requirements

The contractor shall ensure compliance with applicable clauses and travel guide requirements prior to traveling to each of the specified travel locations. The contractor shall be responsible for knowing and understanding all travel requirements as identified by the applicable combatant command (CCMD) and country. The contractor shall be responsible for submitting applicable deployment forms and/or deployment packages (CDRL T025) to the COR or task order technical POC and NIWC Atlantic Deployment Manager no later than 30 days prior to travel. For all OCONUS travel, the contractor shall submit an official OCONUS Travel Form (SPAWARSYSCENLANT 12990/12) and shall ensure all OCONUS travel has an approved Aircraft and Personnel Automated Clearance System (APACS) request. The task order COR will provide a blank travel form after task order award.

11.2.2 OCONUS Immunization Requirements

Pursuant to DoDI 6205.4, SPAWARSYSCENLANTINST 12910.1B, and any additional DON specific requirements, contractor employees who deploy to OCONUS locations both shore and afloat shall require up to date immunizations.

11.2.3 Letter of Authorization

If work requires contractor personnel to process through a deployment center or to travel to, from, or within the designated operational area, the contractor shall have a letter of authorization (LOA) signed by the designated Contracting Officer. The LOA identifies any additional authorizations, privileges, or Government support that contractor personnel are entitled to under task order. The contractor shall initiate a LOA for each prospective traveler. The contractor shall use the web-based Synchronized Pre-deployment & Operational Tracker (SPOT) or its successor, at http://www.dod.mil/bta/products/spot.html, to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary and if in the Government's interest, the contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs are required to be signed and approved by the SPOT registered Contracting Officer of this task order.

12.0 SAFETY ISSUES

12.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the task orders. Without Government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system. If performing within Government facilities, contractor shall immediately report any accidents involving Government or contractor personnel injuries or property/equipment damage to the Contracting Officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the COR or on-site Government representative.

13.0 SUBCONTRACTING REQUIREMENTS

1 APPROVED SUBCONTRACTORS

ıccordance with FAR clause 52.244-2, prior to a prime contractor utilizing a subcontractor, the subcontractor is required to be approved by the ıtracting Officer at the basic contract. As a team member, the subcontractor may be proposed on any upcoming task order competition but is automatically approved for use on any pre-existing task order. After task order award, the prime contractor shall submit a written request to Contracting Officer requesting approval to add any new subcontractors.

proved: (b)(4)

0 ACCEPTANCE PLAN

pection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the QASP, Attachment 1.

0 OTHER CONDITIONS/REQUIREMENTS

1 EXTENDED WORK WEEK

e to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended work week VW) may be required for professional (i.e., salaried) employees.

2 NON-DISCLOSURE AGREEMENT (NDA) REQUIREMENTS

contractor personnel who receive or have access to proprietary information shall sign and abide by a non-disclosure agreement (Attachment 2).

3 FUNDING ALLOCATION

s task order is funded with multiple appropriations with various Accounting Classification Reference Numbers (ACRNs) which may or may not ss multiple contract performance years. Depending on the services performed and the applicable timeframe, the contractor shall invoice cost in ordance with Section B and Section G of the task order award. Unless otherwise advised, the contractor shall itemize all summary of work and ıncial information in the TOSR CDRL by each task order funding CLIN. The ability of the contractor to perform adequate billing and accounting l be reflected in the contractor’s annual Government CPAR rating.

0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

e contractor shall ensure all work accomplished utilizes the latest, relevant industry practices and standards when applicable unless otherwise icated by text. In accordance with Defense Acquisition Policy, maximum utilization of non-Government standards will be made wherever ctical.

1 REQUIRED DOCUMENTS

e contractor shall utilize the following mandatory documents in support of this task order. The documents referenced in this section the minimum version dates; however, the contractor shall meet requirements for any referenced document including subsequent updates applicable at time the task order request for proposal is posted.

	Document Number	Title
a.	DoD 5200.2-R	DoD Regulation – Personnel Security Program dtd Jan 87 (and subsequent revisions)
b.	DoDM 5200.01	DoD Manual – Information Security Program Manual dtd 24 Feb 12
c.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12
d.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
e.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06
f.	DoDI 5220.22	DoD Instruction – National Industrial Security Program (NISP) dtd 18 Mar 11
g.	DoDI 6205.4	DoD Instruction – Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense dtd 14 Apr 00
h.	DoDD 8140.01	DoD Directive – Cyberspace Workforce Management dtd 11 Aug 15
i.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14
j.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14
k.	DoD 8570.01-M	DoD Manual – Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 (and subsequent revisions)
l.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 22 Feb 16
m.	SECNAV M-5239.2	Secretary of the Navy Manual – DON Information Assurance Workforce Management Manual dtd May 2009 (and subsequent revisions)
n.	SECNAV M-5510.30	Secretary of the Navy Manual – DoN Personnel Security Program dtd Jun 2006
o.	SECNAV M-5510.36	Secretary of the Navy Manual – DoN Information Security Program dtd Jun 2006
p.	SECNAVINST 4440.34	Secretary of the Navy Instruction – Implementation of Item Unique Identification within the DoN dtd 22 Dec 09
q.	SECNAVINST 5239.3B	Secretary of the Navy Instruction – DoN Information Assurance Policy dtd 17 Jun 09
r.	SECNAVINST 5239.20A	Secretary of the Navy Instruction – DON Cyberspace IT and Cybersecurity dtd 10 Feb 16
s.	SECNAVINST 5510.30	Secretary of the Navy Instruction – DoN Regulation – Personnel Security Program dtd 6 Oct 06
t.	SPAWARINST 3432.1	Space and Naval Warfare Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
u.	SPAWARINST 4440.12A	Space and Naval Warfare Instruction – Management of Operating Materials and Supplies (OM&S), Government Furnished Property (GFP), and Inventory
v.	SPAWARINST 5721.1B	Space and Naval Warfare Instruction – Section 508 Implementation Policy dtd 17 Nov 09
w.	SPAWARSYSCENLANTINST 3070.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Operations Security Policy dtd 20 Jan 17
x.	SPAWARSYSCENLANTINST 12910.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Deployment of Government and Contractor Personnel Outside the Continental Unlisted States dtd 23 Aug 16

	Document Number	Title
y.	COMUSFLTFORCOM/COMPACFLTINST 6320.3A	Commander US Fleet Forces Command/Commander US Pacific Fleet Instruction, Medical Screening For US Govt Civilian Employees, Contractor Personnel, and Guests prior to embarking Fleet Units dtd 7 May 13
z.	Navy Telecommunications Directive (NTD 10-11)	System Authorization Access Request (SAAR) - Navy
aa.	Privacy Act of 1974	United States federal law, Pub.L. 93–579, 88 Stat. 1896, dtd December 31, 1974, 5 U.S.C. § 552a

16.2 GUIDANCE DOCUMENTS

The contractor shall utilize the following guidance documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the document's effective date of issue is the task order's request for proposal issue date.

	Document Number	Title
a.	MIL-HDBK-61A	Configuration Management
b.	MIL-STD-130N	DoD Standard Practice – Identification Marking of US Military Property
c.	MIL-STD-881C	Work Breakdown Structure for Defense Materiel Items
d.	MIL-STD-1916	DoD Test Method Standard – DoD Preferred Methods for Acceptance Of Product
e.	DoDM 1000.13-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle, Volume 1, dtd 23 Jan 14
f.	DoDI 3020.41	DoD Instruction – Operational Contract Support (OCS) dtd 20 Dec 10
g.	DoDI 4161.02	DoD Instruction – Accountability and Management of Government Contract Property dtd 27 Apr 12
h.	DoDD 5000.01	DoD Directive – The Defense Acquisition System
i.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System
j.	N/A	Guidebook for Contract Property Administration dtd Dec 2014
k.	NAVSEATS9090-310F	NAVSEA Technical Specification 9090-310 dtd 12 Feb 15 (and subsequent revisions)
l.	ISO 9001 (ANSI/ASQ Q9001)	International Organization for Standardization (American National Standard Institute/American Society for Quality) – Quality Management Systems, Requirements
m.	ISO/IEC 12207	International Organization for Standardization/ International ElectrotechnicalCommission: Systems and Software Engineering – Software Life Cycle Processes
n.	ISO/IEC/IEEE 15288	International Organization for Standardization/ International ElectrotechnicalCommission: Systems and Software Engineering – System Life Cycle Processes
o.	ASTM Std E-2135-06	American Section of the International Association for Testing Materials, Standard
p.	IEEE Std 12207-2008	Institute of Electrical and Electronics Engineers – Systems and Software Engineering, Software Life Cycle Processes
q.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors dtd 27 Aug 04

	Document Number	Title
r.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
s.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification
t.	N/A	NAVSEA Standard Items (NSI) – http://www.navsea.navy.mil/
u.	N/A	NIWC Atlantic Contractor Check-in portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/Contractor+Checkin
v.	N/A	COMSPAWARSYSCOM Code 80330 mandatory training webpage – https://wiki.spawar.navy.mil/confluence/display/HQ/Employee+Mandatory+Training
w.	N/A	DoD Foreign Clearance Guide – https://www.fcg.pentagon.mil/fcg.cfm

16.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents necessary for performance on this task order. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.

-

[END OF PWS]

PERSONNEL QUALIFICATIONS (MINIMUM)

(a) Personnel assigned to or utilized by the contractor in the performance of this contract shall, as a minimum, meet the experience, educational, or other background requirements set forth below and shall be fully capable of performing in an efficient, reliable, and professional manner.

(b) The Government will review resumes of contractor personnel as required during performance of the contract/task order.